MCWP 3-40.5

ELECTRONIC WARFARE

U.S. Marine Corps

Coordinating Draft 23 April 2001

PCN 144 XXXXXX XX

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-0001

DATE

FOREWORD

1. PURPOSE

Marine Corps Warfighting Publication (MCWP) 3-36.1, *Electronic Warfare,* updates present doctrine for employment and use of electronic warfare in support of the Marine Air-Ground Task Force (MAGTF).

2. SCOPE

This manual presents provides an overview of electronic warfare doctrine, tasks, and structure in MAGTF and joint/multi-national operations. It is not exclusively for personnel who work within the field of electronic warfare.

3. SUPERSESSION

Fleet Marine Force Manual (FMFM) 7-12, *Electronic Warfare,* dated 20 May 1991.

5. CERTIFICATION

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

B.B. KNUTSON JR.
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command
Quantico, Virginia

MCWP 3-36.1, *ELECTRONIC WARFARE*

Table of Contents

Appendix

A. EW Support Capabilities and Support Activities
B. JOPES format for EW Guidance
C. JOPES format for EW OPORD Appendix
D. Joint EW Reports

CHAPTER 1

ELECTRONIC WARFARE OVERVIEW

Purpose

This chapter will introduce the importance, basic concepts, and definitions that relate to Electronic Warfare.

Introduction

The modern battlespace has become more sophisticated. Military operations are executed in an increasingly complex electromagnetic (EM) environment. Military forces, as well as civilians, depend on electronic equipment operating within the electromagnetic spectrum for communications, navigation, information gathering, processing, and storing; and as a means for detection and identification of enemy forces. Historically, radar has been the primary concern of electronic warfare; today the threat has expanded to include command and control systems, electro-optic systems, electromagnetic dependent munitions, and directed energy systems.

The outcome of modern conflict greatly depends on control of the electromagnetic spectrum. The force that selectively deprives the enemy of the use of the electromagnetic spectrum, or exploits its use by the enemy to obtain information, has an important advantage.

Adversaries possess the full range of modern communications, surveillance, and weapon systems that operate throughout the EM spectrum. They are aware of the threat posed by our own EW resources. In general, all sides will attempt to dominate the EM spectrum by targeting, exploiting, disrupting, degrading, deceiving, damaging, or destroying their opponents electronic systems which support military operations will retaining their ability to make use of the same systems.

Modern warfare demands that each echelon of command effectively use the electromagnetic (EM) spectrum for their purposes while preventing its effective use by the enemy. In this context, EW is an important part of the arsenal of responses available to military commanders. However, the effective use of EW can only be achieved through close coordination with other resources deployed in support of military operations.

EW doctrine provides a basis for:

- Effective integration of EW within the MAGTF
- Coordination and cooperation between joint force components, particularly for the effective employment of EW resources.
- Operational, procedural, and technical interoperability at operational and tactical levels.
- The exchange of EW related information and intelligence between US forces and allied nations or coalition partners.

Electronic Warfare Definitions

The concepts and doctrine for EW are derived from a series of definitions that, in general terms, explain the boundaries of EW

activities. The central definition for EW, from which subordinate definitions are derived, is defined as:

> *Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (Joint Pub 1-02)*

The definition of EW can be broken down into three key components: exploitation, disruption, and denial. These three components give rise to the following activities:

a. Electronic Warfare Support (ES)
b. Electronic Attack (EA)
c. Electronic Protection (EP)

a. Electronic Warfare Support

Electronic Warfare Support (ES) is defined as:

> *That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. (Joint Pub 1-02)*

ES provides information required for decisions involving EW operations and other tactical actions such as threat avoidance, targeting, and homing. ES systems collect data and produce information or intelligence that can be used to:

a. Corroborate other sources of information or intelligence
b. Direct EA operations
c. Initiate self-protection measures
d. Task weapon systems for physical destruction
e. Support EP efforts
f. Create of modify EW databases
g. Support Information Operation (IO) activities

ES data can be used to produce signals intelligence (SIGINT), provide targeting for electronic or destructive attack, and produce measurement and signature intelligence (MASINT). See Marine Corps Warfighting Publication (MCWP) 2-15.2, *Signals Intelligence*.

ES systems provide immediate threat recognition and a source of information for immediate decisions involving EA, EP, avoidance, targeting, and other tactical employment of forces.

ES and SIGINT involve searching for, intercepting identifying, and locating sources of intentionally or unintentionally radiated electromagnetic energy. The primary difference between the two is the detected information’s intended use, the degree of analytical effort expended, the detail of information provided, and the timelines required. ES is conducted for immediate threat recognition, and provides information required for immediate tactical decisions. SIGINT is used to gain information concerning the enemy, usually in response to an intelligence requirement.

The ES intelligence collection effort can be characterized as follows:

a. It is used in peace, crisis, and war. Its peacetime collection efforts make an essential contribution tot he building of an intelligence/EW database for planning and operations.

b. It provides an all weather, day/night, long-range information gathering capability.

c. It exploits an adversary's EM emissions and may provide information of adversary capabilities and intentions.

d. It is covert and passive.

e. It is a non-intrusive method of intelligence collection.

b. Electronic Attack (EA)

Electronic Attack (EA) is defined as:

> *That division of electronic warfare involving the use of electromagnetic, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. (Joint Pub 1-02)*

Some common types of EA are spot, barrage, and sweep jamming; but also include various electromagnetic deception techniques, such as repeaters, transponders, reflectors, and chaff.

Directed energy (DE) is an umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. A DE weapon is a system using DE primarily as a direct means to damage or destroy adversary equipment, facilities, and personnel.

Anti-radiation weapons are simply those types of weapons that use radiated energy as their mechanism for guiding onto a targeted emitter.

c. Electronic Protection (EP)

Electronic Protection (EP) is defined as:

> *That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. (Joint Pub 1-02)*

Generally, the measures included under the heading of EP are also included under the heading of good communications procedures. If communications are properly planned and executed, many of the measures needed to minimize the vulnerability of friendly units to enemy EA and ES will be accomplished. Similarly, if the use of non-communications electronic equipment (such as radar and data links) is properly planned and executed, many of the measures needed to minimize the vulnerability of units that depend on those equipments will be accomplished.

The technical aspects of EP must be considered when equipment acquisition programs are initiated. Additionally, these programs must be reviewed when EA vulnerabilities are detected.

In combat, EP is practiced through the application of good training and sound procedures for countering enemy EA. All operators, users, and planners of electronic equipment must thoroughly understand the threat and the vulnerability of their equipment to enemy EA efforts and ensure that they take appropriate actions when attacked.

EP measures include the selection of a scheme of maneuver that will minimize friendly electronic emissions that the enemy can intercept or disrupt using his ES and EA capabilities. This can be done by, among other ways, having a simple scheme of maneuver which can be executed with few or no emissions, by imposing radio silence or emission control (EMCON) procedures, or by selecting avenues of approach which will interpose terrain between friendly transmitters and enemy intercept stations. EP also includes measures to minimize the vulnerability of friendly receivers to enemy jamming. These may include use of reduced power, brevity of transmissions, and directional antennas.

To minimize an adversary’s opportunity for successful ES and EA operations against US forces, it is necessary to:

a. Regularly brief the EW threat to force personnel

b. Provide training on appropriate EP responses.

c. Ensure that electronic system capabilities are safeguarded during exercises, work-ups, and pre-crisis training.

EW and Spectrum Management

Military operations occupy battlespace comprising sea, land, air, space, and the electromagnetic spectrum. Conflict may take place in all of these domains. Management of own forces and resources within the electromagnetic domain is a major task. Spectrum management plays a key role in the successful planning and execution of EW. EW activities are coordinated and de-conflicted through the Electronic Warfare Coordination Center (EWCC). The primary mechanism for spectrum management is the Restricted Frequency List (RFL).

CHAPTER 2

ELECTRONIC WARFARE PLANNING

Purpose

The purpose of this chapter is to provide a basic description of electronic warfare (EW) planning, explain its relationship to the Marine Corps Planning Process (MCPP), and present EW operational planning considerations for: ES, EA, and EP planning; EW deception planning; and for EW in support of Suppression of Enemy Air Defense (SEAD).

EW Planning Overview

Synchronization of EW

The MAGTF campaign is the synchronization of air, land, sea, space, and special operations in harmony with diplomatic, economic, and informational efforts to attain national objectives. By its nature, information operations (IO) planning must be broad-based and encompass all IO functions (EW, OPSEC, PSYOPs, physical destruction, deception, computer network operations) and the employment of all available IO resources (joint, Service, interagency, multinational). IO requires early integration within the MAGTF and with external agencies. EW planning occurs is coordinated with other information operation activities and is planned simultaneously with operational planning.

Planning for EW Employment with the OPORD

a. EM Spectrum Management. Since EW takes place in the electro-magnetic (EM) spectrum, EW planners must closely coordinate their efforts with those members of the staff who are concerned with managing military use of the EM spectrum. The Joint Restricted Frequency List (JRFL) is a key tool for spectrum management.

b. EW Planning Guidance. Planning guidance for EW should be included in the OPLAN as a tab to the IO guidance. IO guidance is normally appended to Appendix 3 (IW) of Annex C (Operations) of the OPLAN.

c. EW Annex. The EW Annex is included as a Tab to Appendix 3 (IW) to Annex C (Operations) of the OPLAN. See Appendix XXX of this publication. The EW Annex should:

- Identify the desired EM profile selected by the commander for the basic concept of operations and provide EMCON guidance to commanders so that desired EM and acoustic profiles are realized.

- Identify EW resources required to support IO, SEAD, and the other elements and activities of IO

- Evaluate enemy threats to critical friendly command and control (C2), communications, weapons control systems, target acquisition systems, surveillance systems, and computer networks, and specify EP measures necessary to ensure effective operations during combat.

EW Planning Factors

Development of the EW portion of the OPLAN requires consideration of a number of diverse factors about the proposed operations. Planning factors include the following.

- Requirements for friendly communications, navigation systems, and radar. These requirements should be considered with respect to the anticipated operations, tactical threat expected, and EM interference considerations. Once identified, these requirements should be entered into the JRFL under appropriate categories (TABOO etc.).

- Identification of COMSEC and electronic security measures necessary to deny OPSEC indicators to enemy passive-EM sensors.

- Development of the Joint Restricted Frequency List (JRFL) is a critical to ensuring deconfliction of EA and ES activities.

- Coordination and identification of specific resources required for interference de-confliction.

- Identification of essential priority intelligence requirements (PIR) that support commanders and EW operations. These PIR must be included in the intelligence annex (normally Annex B) of the OPLAN to facilitate ES.

- Coordination and establishment of procedures to ensure timely fulfillment, including tactical real-time dissemination.

- Review of ROE to determine what restrictions (if any) may be placed on EW operations.

The Marine Corps Planning Process

The Marine Corps Planning Process (MCPP) is an internal planning process used by Marine Corps operating forces. It aligns with and complements the joint deliberate and crisis action planning process. The MCPP is applicable across the range of military operations and is designed for command and staff actions at any echelon of command.

The MCPP establishes procedures for analyzing a mission, developing and wargaming courses of action (COAs) against the threat, comparing friendly COAs against the commander's criteria and each other, selecting a COA, preparing an operation order or operation plan for execution, and transitioning the order or plan to those tasked with its execution. The MCPP organizes these procedures into six manageable, logical steps (see Figure XXX).

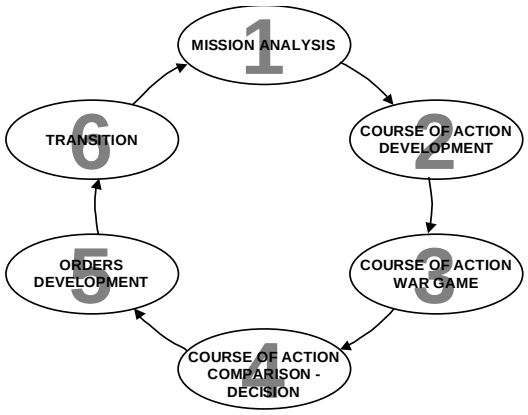

Figure XXX, Marine Corps Planning Process

MCPP and EW Planning

The EW plan is developed in conjunction with other MAGTF operational maneuver concepts. EW planning is normally accomplished by the Electronic Warfare Coordination Center (EWCC) and is led by the G/S-3 staff Electronics Warfare Officer (EWO) with representatives from the G/S-2 and G/S-6. EW planning occurs concurrently with other operational planning within the Marine Corps Planning Process.

MCPP Step	EW Planning Action
Mission Analysis:	Review Commander's Guidance Review Rules of Engagement (ROE) Identify CCIR/PIR/EEFI Coordinate internal liaison Request external augmentation as required Identify adversary operational centers of gravity (COG) Develop the EW Estimate Produce the EW Mission Statement Determine EA, ES, and EP objectives
COA Development:	Conduct Intelligence Gain/Loss (IGL) review Consider Special Information Operations (SIO) Model EW effects Integrate with operational maneuver Determine command relationships
COA Wargame:	Utilize automated models Wargame in conjunction with other IO COAs
Comparison/Decision:	Brief MAGTF Commander and G/S-3
Orders Development:	Develop Electronics Warfare TAB TO APPENDIX 3 (IW) to ANNEX C (OPERATIONS)
Transition:	Publish OPORD Integrate ES into MAGTF intelligence cycle Integrate ES and EA into MAGTF targeting cycle Integrate ES and EA into MAGTF Battle Damage Assessment (BDA) cycle Monitor/control EW operations

Planning for EW Operations

Planning Considerations for Electronic Warfare Support (ES)

a. Intelligence Support to ES. Accurate electronic order of battle information must be available in order to accurately program ES equipment, such as radar warning and tactical jamming systems.

b. ES Support to Intelligence. Detected information derived from ES equipment can be rapidly disseminated should significant threats be encountered. Processing and analysis of recorded ES information requires a varying yet generally longer time before dissemination. At this point, ES generally enters the arena of intelligence.

ES is part of the overall intelligence effort. Thus, the information acquired by ES activities is disseminated through the same channels as

intelligence, target data, and combat information. Indeed, information acquired through ES activities is usually blended with other information or otherwise made to appear that it was acquired by other than ES activities. Further, ES support is usually not requested as such.

Exceptions to the above occur when EW collection assets can pass ES and other information directly to a unit. Examples of this are the providing of a SIGINT support unit (SSU) from radio battalion to a headquarters or the passing of TERPES-generated reports to various headquarters. In these cases, specific types of plans must be developed. VMAQ post mission reports are automatically generated and submitted to MAGTF and other units, as directed by the MAGTF commander. TERPES can also provide EW and intelligence products in response to requests from other units in accordance with procedures established by the MAGTF commander. Since the TERPES automatically disseminates reports, recurring requirements for the information promulgated in TERPES reports should be requested as far in advance as possible.

Planning Considerations for Electronic Attack

General

EW operations must effectively support combat operations. To achieve this, the EW plan must be developed early, it must be fully integrated into the overall operational plan, and it must be continually updated in light of changes in the tactical situation. The need for updating is important. If the EW plan is not adjusted as the situation changes, ES may not provide the needed types of information, and electronic attack may have an adverse effect on friendly command, control, and communications. EW must be coordinated at all levels and among US forces and participating allies.

1. Authorization. The results of EW can be profound and far-reaching, not only at the tactical level, but also at the operational and strategic level. EW planners and operators must understand both peacetime and wartime rules of engagement (ROE).

2. Jamming Control. Because of its possible impact on friendly communications and non-communications emitters (e.g., radars and data links), jamming will normally require centralized control (authority). However, in certain situations, control (authority) may be delegated to lower commanders.

3. Timing. Jamming may only be effective for a limited time because the enemy may attempt to use electronic protection to overcome jamming effects. To be effective, jamming must be brought to bear quickly at the critical time and place. Maximum effectiveness will be obtained if the attack is delivered at a critical time against a critical enemy electronic system (e.g., fire control nets during his attack, air defense systems during friendly offensive air operations, command and control communications for the control of the movement or commitment of reserves).

Jamming may be preplanned or in response to an immediate tactical situation. In deciding upon electronic jamming, commanders and staffs must carefully weigh the operational requirement against the restrictions or effects imposed on friendly systems and the loss of information about the enemy otherwise obtained by electronic warfare support measures. Degradation of some friendly command and control communications may have to be accepted in order to effectively employ jamming. Jamming's greatest weakness is that it may indicate to the enemy what we know about the frequencies he is using. And knowing

this, he may change his frequencies, if capable, making further jamming difficult and making ES much less productive.

Jamming, like all warfare techniques, is most effective when used against an enemy who is not prepared for it. Jamming for the purpose of harassing the enemy or gaining or supporting a minor operation is usually counterproductive because it assists the enemy in determining his vulnerability to jamming and because it helps his operators learn to recognize our jamming and to work through it. Jamming is usually effective for a limited time only. The enemy usually will take whatever measures are necessary to overcome the effects of jamming.

EA Employment Considerations

To jam, the frequencies being used by the target stations must be known and a favorable jamming-to-signal ratio (JSR) must be achieved over the receiving station. A favorable JSR means the jamming signal received at the target-receive antenna is stronger than the enemy signal intended for that same target-receive antenna. This ratio is influenced by the location and effective radiating power of the jammer, the terrain and distance between the jammer and the station being jammed, and the characteristics of the jammers antenna and the target's antenna.

a. EA limitations. These include the need for information on the structure of enemy radio nets and on the frequencies he is using (a technical data base). Another limitation is compromising the technical database. The enemy may change the frequencies of the nets we jam. If the enemy uses the same frequencies for his important nets which we use for our important nets, EA may be impossible. The provision of backup frequencies can overcome this problem.

b. Mutual Support. Jamming should be recognized as a complementary option to attack the enemy where other methods, such as fire support, are not more suitable or are not available. Jamming operations must be integrated into overall attack planning. Jamming is a means to an end, not an end in itself. Some of the activities jamming can support include:

- Disrupting command and control by impeding or disrupting communications and data links between elements of a force; denying or delaying radar early warning, ground control intercepts and target acquisition and tracking; and defeating or degrading critical links inherent in surface-to-surface and surface-to-air weapons systems (missile beacons or seekers).
- Intelligence collection by prompting a unit to transmit in the clear rather than over secure communications circuits.
- Causing communication or noncommunication equipment shortages by making it appear that radio, data link, teletype, and radar equipment are not operating properly.

Indiscriminate employment of jamming must be avoided. The best results are obtained when resources are concentrated to simultaneously disrupt or degrade all types of electromagnetic communications and/or non-communications systems (e.g., radar and datalinks) of selected enemy units, formations, or weapons systems that have a direct impact on the accomplishment of our mission.

Developing the EA Plan

Usually, a commander requesting EA support should describe only the operation to be supported and not attempt to list the frequencies and stations to be jammed. The object of EA operations is to disrupt the enemy's command and control while some important tactical evolution is occurring. EA operations should reduce the enemy's combat power when we can best exploit this reduction. Communication systems are usually complex and provide several channels for passing requests for fires, requests for reinforcements, intelligence reports, and other critical messages. Thus, for example, an EA plan which is intended to disrupt radio communications between an enemy unit and a supporting artillery unit must disrupt more than the nets used by enemy forward observers to request fire support.

Requests for EA support are forwarded through the chain of command to the commander authorized to plan and conduct EA operations. For operations involving assets of the radio battalions, this is usually the MAGTF commander. For airborne EA support by EA-6Bs, this is usually the ACE commander. The commander authorized to conduct EA makes a tentative decision on whether or not to provide the requested support. This tentative decision is based on such things as the relative importance of the tactical activity being supported, competing requests, and the adequacy of the technical data base. If a tentative decision is made to provide the requested EA support, the request is passed to the supporting EW unit.

Staffing the EA Plan

1. Attached units. EA plans developed by EW units attached to the MAGTF headquarters or to one of its elements are submitted to the Electronic Warfare Coordination Center (EWCC). The Electronic Warfare Officer (EWO) staffs these plans within the headquarters and with adjacent, supporting, and higher headquarters. The Communications-Electronics Officer (CEO) reviews the plans to ensure that they will not disrupt command and control communications. The G-2 reviews the plans to ensure that they will not needlessly disrupt or stop collection of critical information and intelligence. Problems which arise during the staffing which cannot be resolved are referred to the commander or his designated representative, usually the G-3. Problems which arise during the staffing of the plan with adjacent, supporting, and higher headquarters must be referred to higher authority for reconciliation. Once all problems are identified and reconciled, the decision will be made whether or not to execute the plan, and if so, when. Usually the assistant chief of staff, G-3 makes the decision.

2. Other units. EA plans developed by adjacent, supported, and supporting headquarters should be coordinated by these headquarters with the MAGTF headquarters. The EWO will be responsible for staffing these plans with the G-2, G-3 and CEO. The headquarters which originated the plan will be advised of the problem and attempts will be made to resolve the problem. Problems which cannot be resolved will be referred to higher authority. The headquarters which originated the plan will also be advised when the staffing has been completed and no problems have been found.

Planning Considerations for Electronic Protection (EP)

a. General. Electronic protection is the subdivision of EW involving actions taken to protect personnel, facilities and equipment from any effects of friendly or enemy employment of EW that degrade, neutralize or destroy friendly combat capability. EP includes physical security, information security (INFOSEC), communications security (COMSEC) measures, and emission control (EMCON) measures. It also includes the

detection and response to hostile action against own force information systems.

b. External Support for EP. Vulnerability analysis and assessment form the basis for formulating EP plans. The Defense Information Security Agency (DISA) operates a program known as the Vulnerability Analysis and Assessment Program (VAAP) specifically focusing on automated information systems. The National Security Agency (NSA) has a communications security (COMSEC) monitoring program that focuses on telecommunications systems using wire and electronic communications.

c. EW Reprogramming. The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW and target sensing systems (TSS) equipment maintained by field and fleet units. EW reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems. The reprogramming of EW and TSS equipment is the responsibility of each Service or organization through its respective EW reprogramming support programs. However, during joint operations, the swift identification and turnaround of reprogramming efforts could become a matter of life and death in a rapidly evolving hostile situation. There is a need for joint coordination of Service reprogramming efforts to ensure that reprogramming requirements are identified, processed, and implemented in a timely manner by all affected friendly forces.

Planning Considerations for Electronic Deception

The employment of electronic deception, like jamming, is integral to staff planning and must support the overall operation plan. Electronic deception on a large scale is expensive in terms of preparation time and resources. For electronic deception to be effective, it must be complemented by sonic, visual, and olfactory deception. The advance in electronic sensor technology and the speed with which information can be transmitted, received, correlated, and displayed for evaluation and decision making makes it extremely difficult to execute a large electronic deception effort with any degree of success. The enemy is likely to discover large deception efforts unless they are planned in detail and supported generously with personnel and equipment. Deception efforts are more likely to succeed if designed to achieve a specific objective that is limited in time and scope. Land forces are, therefore, more likely to make use of limited scale deception operations at selected key times in the battle. Electronic deception should be conducted as part of an overall deception plan.

(a) Coordination and Control. Deception operations, like jamming, normally require centralized coordination and control. . Missions are normally preplanned but may be immediate if opportunities for limited application become available.

(b) Imitative Electronic Deception (IED). IED, which involves the transmission of false voice commands to enemy units, requires personnel who are exceptionally fluent in the enemy's language; i.e., can use enemy dialects, slang, and terminology. The availability of such personnel must not be taken for granted. IED varies in scope based on the sensitivity of the intelligence and the sophistication of techniques and equipment used. It could include nuisance intrusion, planned message intrusion, cryptographic intrusion, or deception intrusion. All but nuisance intrusion require extensive technical support and specially skilled operators. Nuisance intrusion requires only compatible radio equipment and foreign language ability. All require specific authorization from the senior headquarters controlling the operation.

Planning Considerations for EW support of SEAD

Suppression of enemy air defence (SEAD) is a specific type of mission intended to neutralize, destroy, or temporarily degrade surface-based adversary air defenses with destructive and/or disruptive means. SEAD is a broad term that includes all SEAD activities provided by one component of the joint force in support of another. SEAD missions are of critical importance to the success of any operation when control of the air is contested by an adversary. SEAD is invariably a high priority mission that relies on a variety of EW platforms to conduct ES, EP, and EA in support. EW planners should coordinate closely with joint and component air planners to ensure that EW support to SEAD missions is integrated into given priority in the overall EW plan. Given the fundamental importance of control of the air in any joint operation involving hostilities, care should be taken that EW assets required for SEAD missions are not allocated to other EW missions, particularly during that portion of an operation when control of the air may be contested.

CHAPTER 3

INTEGRATION OF ELECTRONIC WARFARE

Purpose

The purpose of this chapter is to describe the relationship of EW to command and introduce various aspects of controlling EW operations. It will also describe various staff roles in the coordination of EW. Finally, this chapter will describe the basic concepts of amphibious and littoral EW, ground and airborne EW, and joint and multi-national EW operations.

EW and Command

There will always be a commander who is assigned overall operational control of all forces engaged in an operation. This commander is the focal point for conducting the operation and his staff is the central coordinating authority. Electronic Warfare falls under the staff cognizance of the Staff Operations Officer (G/S-3). The commander and his staff will be supported by the Electronic Warfare Coordination Cell (EWCC). Its composition is dictated by the size of the force, the mission, and the EW resources available. All EW activities for the MAGTF are coordinated through the EWCC. EW participation in information operations will be accomplished through the EWCC.

Although EW is coordinated through the EWCC, the employment of EW is a function of command. EW units have responsibilities that include:

a. Developing an EW concept of operations
b. Planning and coordinating EW related activities
c. Developing supporting plans
d. Supporting operational maneuver of the MAGTF
e. Synchronizing ES, EA, and EP activities

EW Control

EW functions are assigned to the staff to assist the commander in his responsibilities for planning and conducting EW operations. Thorough and continuous coordination is necessary to ensure that EW that is employed against an enemy threat will not unacceptably degrade friendly use of the EM spectrum. The MAGTF Commander will normally plan, synchronize, coordinate, and de-conflict EW operations through the electronic warfare coordination center (EWCC).

The EWCC

The EWCC facilitates coordination of electronic warfare operations with other fires and communications and information systems. The EWCC is under staff cognizance of the G-3. It coordinates efforts by the G-2, G-3, and G-6 to eliminate conflicts between mutually supporting battlespace functions. Assigned personnel identify potential conflicts in planned operations and work to resolve these issues. The EWCC may include an electronic warfare officer, a communications and information systems representative, and other liaison officers as needed. Liaison could include radio battalion representation, airborne electronic

countermeasures officers, a MACG radar officer, and other-Service representatives.

MAGTF staffs will provide personnel to incorporate an EWCC with the G/S-3. Personnel will also be provided for liaison teams to higher headquarters EW coordination organizations when required, such as the Joint Commander’s Electronic Warfare Staff (JCEWS) created by Joint Task Forces (JTFs).

EWCC Structure

The structure of the EWCC is determined by several factors such as the overall structure of the combatant force and the level of EW to be conducted. The EWCC is ‘type’ structure upon which to build Marine EW functions. It does not add structure to the existing organization, but rather is used to coordinate EW activities of personnel already assigned.

a. Highly complex Joint Suppression of Enemy Air Defense (JSEAD) operations may require the command’s EW staff to coordinate with representatives from the Air Force, Army aviation, Navy, air defense, manuever units, and artillery to plan and execute the operation.

b. A limited jamming operation may be managed by the EW staff with minimum outside coordination required.

EWCC Functions and Responsibilities

a. Coordinates, synchronizes, and de-conflicts EW targeting with fire support and intelligence collection plans and operations

b. Ensures that EW is considered in each phase of the OPLAN/OPORD

c. Integrates EW into the IO portions of OPLANs/OPORDs

d. Ensures the command’s EW operations support the JTF campaign plan

e. Recommends to the G-3 the level of EW taking of subordinate commands

f. Assists the G-6 in the compilation of the Restricted Frequency List (RFL) and the Joint Restricted Frequency List (JRFL)

g. Resolves potential EW fratricide and misidentification issues

h. Coordinates subordinate command’s request for EW support

i. Coordinates requests for EW support from other services and allies

j. Establishes procedures for the rapid exchange of EW information to support planning and execution

k. Assesses the effects of friendly and enemy EW activity on the battlefield

l. Maintains the status of EW resources available to the commander

m. Identifies EW requirements for intelligence support

n. Coordinates EW reprogramming activities

o. Coordinates the administrative and logistical support, and communications requirements of tailored EW packages in the Time-Phased Force and Deployment Data (TPFDD)

EW Control Tasks

Control of EW operations is essential to allow optimal friendly use of the electromagnetic spectrum while targeting the enemy in a manner that supports the operational maneuver. However, control may be made difficult in joint operations or operations involving the participation of allied forces. EW is broadly controlled by establishing measures to ensure the coordination of EW activities between forces, establishing procedures to monitor the execution of EW activities, and finally by establishing a means to assess the effectiveness of EW operations and to recommend and implement changes.

1. Coordinate EW operations

a. Within the parameters of designated authority
b. Direct action within established timelines and conditions
c. Coordinate actions and operations, where lines of authority and responsibility overlap or conflict
    (1) Advises units of adjacent or related actions and operations
    (2) Directs supporting operations
    (3) Resolves conflicts

d. Coordinate continuing support for EW operations
    (1) Coordinate administrative support
    (2) Coordinate logistical support
    (3) Coordinate communication support
    (4) Coordinate external agency support (i.e. JCMA, JSC, JIOC)

2. Monitor EW operations

a. Monitor Electronic warfare Support (ES)
    (1) Execution in accordance with SIGINT operational tasking authority
    (2) Provides information, or feedback, for analysis of the effectiveness of information operations (IO)
    (3) Monitor dissemination of ES to support EA and EP
b. Monitor EA operations
    (1) Maintain positive control of EA operations
    (2) Ensure integration with targeting process
c. Monitor EP operations
    (1) OPSEC assessment and plan
    (2) COMSEC monitoring operations
    (3) EW Reprogramming, as required

d. Coordination
    (1) Deconflict EA operations with Joint Restricted Frequency List (JRFL)
    (2) Crosswalk with planned IO (including deception, destruction, PSYOP, OPSEC)

3. Assess effectiveness of EW operations

a. Electronic Warfare Support (ES)
    (1) Search for, intercept, identify, and locate sources of radiated electromagnetic energy
    (2) Provide near real-time (NRT) threat recognition in support of immediate operational decisions involving EA, EP, avoidance, targeting, or other tactical employment of forces
b. Electronic Attack (EA)
    (1) Focus on offensive use of electromagnetic spectrum to directly attack enemy combat capability
    (2) Coordinate EW with military deception plans (timing, message, feedback mechanism)
    (3) Use of directed energy and anti-radiation missiles
c. Electronic Protection (EP)
    (1) Protect personnel, facilities, equipment from effects of friendly or enemy EW
    (2) Employ communication security (COMSEC) measures
    (3) Employ emission control (EMCON) measures
    (4) Employ war reserve modes (WARM)
    (5) Reassess operational and tactical measures and countermeasures
    (6) Coordinate EW Reprogramming

4. Maintain EW estimate

a. Review/revise EW Course of Action (COA) in support of current and future operations
    (1) In coordination with G-2, Intelligence
    (2) Integrate EW in targeting cycle
    (3) Integrate ES in battle damage assessment (BDA)
    (4) Integrate EW into fires plans
b. Review/revise EA COA
    (1) Integrate electromagnetic deception in support of military deception, as required
    (2) Review operational effect of tactical jamming and destructive EA
    (3) Submit targets for re-strike, suppression as required
c. Review/revise EP COA
    (1) Integrate EW with OPSEC and SIGINT efforts
    (2) Coordinate EW with RFL/JRFL
d. Wargame EW COAs

5. Recommend changes to EW operations

a. Ensure EW operations maintain currency with MAGTF Commanders' Intent
b. Coordinate EW operations with tactical operations
c. Integrate EW within scope of Information Operations

Coordination between the MAGTF Staff and the EWCC

Operations Staff (G/S-3) to the EWCC

The Operations Staff has the responsibility for planning, coordinating, and supervising EW activities, except for intelligence aspects. The operations staff is responsible for:

a. Exercising EW on the behalf of the commander, through the issuance of operations orders.

b. Tasking assigned and attached EW units through the EWCC.

c. Exercising control over EA, including integration of electronic deception plans.

d. Coordinating EW training with other requirements.

Intelligence Staff (G/S-2) to the EWCC

The intelligence staff advises the commander and his staff on the intelligence aspects of EW. The intelligence staff is responsible for:

a. Tasking EW units in accordance with the intelligence collection plan.

b. Providing intelligence on enemy organizations, locations, and capabilities.

c. Assisting in the preparation of intelligence related portion of the EW estimate.

d. Disseminating EW intelligence.

e. Provide advice on the RFL by recommending GUARDED frequencies.

f. Maintain appropriate EW databases.

Communications-Electronics Staff (G/S-6) to the EWCC

The Communications-Electronics Staff is the coordinator of the EWM spectrum for a wide variety of communications and electronics resources. It is responsible for:

a. Issuing Communications-Electronics Operating Instructions (CEOI).

b. Preparing EP policy on behalf of the Commander.

c. Coordinate the preparation of the RFL and issuance of EMCOM guidance.

d. Assisting in the preparation of EW plans and annexes.

e. Coordinating frequency allocation, assignment, and use.

f. Coordinating electronic deception plans and operations in which assigned communication resources participate.

g. Coordinate measures to reduce electronmagnetic interference.

h. Reporting all enemy EA activity to the EWCC for counter-action.

Information Operations Cell and the EWCC

The Information Operations (IO) Cell coordinates EW activities with other information operation activities in order to maximize effect and prevent mutual interference. An EWCC representative may be assigned to the IO Cell to facilitate coordination.

The Operations Control and Analysis Center and the EWCC

The Operations Control and Analysis Center (OCAC) provides centralized direction, management, and control of SIGINT and ground EW activities within the MEF and coordinates with the MEF EWCC and external national assets. Assigned personnel process, analyze, and disseminate collected information. The OCAC is located within the MEF Headquarters near other intelligence agencies. The OCAC provides an interface between the radio battalion and the MEF G-2. The OCAC coordinates ground EW activities with the EWCC.

Amphibious and Littoral EW

In amphibious operations, the planning and conduct of EW operations is the responsibility of the Commander, Amphibious Task Force (CATF). While afloat, the Commander Landing Force (CLF) is subordinate to the CATF. Under these circumstances, the CLF will conduct only those EW operations specifically assigned by the CATF. In joint operations, the CATF will coordinate his EW plans and operations with the Joint Force Commander (JFC) through the Joint Commander’s Electronic Warfare Staff (JCEWS).

Subject to the overall authority of the CATF within the area of operations, the CLF is responsible for the conduct of landing force EW operations ashore. The initiating directive may nevertheless require that coordination of EW operations be retained afloat or transferred to an EWCC of an appropriate headquarters ashore, as required by the local situation.

The CLF will designate a landing force EW Officer who will be responsible to the coordination and control of EW operation ashore and for the preparation of the EW input to the landing force operation plans and orders.

When the CATF and CLF are embarked in the Amphibious Task Force (ATF) a landing force EWCC may be established afloat to coordinate EW plans and operations with the naval Electronic Warfare Coordinator (EWC). When the landing force moves ashore, the EWC will continue to function in support of CATF and the EWCC will function in support of the CLF. However, close coordination of EW operations remains necessary.

Ground Electronic Warfare

a. General. Ground EW is used to support the GCE and operational maneuver, it is used as the MAGTF commander deems necessary. Generally, ground EW equipment is employed on highly mobile platform. Where possible, this equipment should have the same mobility and survivability as the supported force. Direction finding and EA sites are usually located in the forward area of the battlefield, with or near forward units due to short-range nature of tactical signals. Ground EW is primarily directed against tactical communications systems.

b. Requirements.

- Protection from enemy ground and aviation elements by the supported unit.
- Logistical support.
- Clear identification of EW requirements of the supported commander.

c. Capabilities.

- Best suited to support operations of ground units.
- Can be positioned to allow continuous operations during enemy attack.
- Responsive to EW requirements of supported ground commander.
- Can support aviation units or the MAGTF in general support (i.e., jamming of enemy air defense and C3 during an air attack in coordination with VMAQ).

d. Limitations.

- Vulnerable to enemy attack.
- Can be masked by terrain.
- Distance/propagation characteristics of enemy electronic systems.
- EP actions employed by the enemy.
- Vulnerable to enemy electronic deception measures.

Airborne Electronic Warfare

a. General. The procedures followed in planning and executing airborne electronic warfare are similar to ground EW units. The most significant difference between ground and airborne EW employment is in terms of time. Aviation operations are generally much shorter in duration and conducted at much higher speeds than ground operations. The timeliness of EW support is critical in aviation operations. It requires a more extensive database and detailed plan than required for ground operations.

b. Characteristics.

- Airborne EA and ES operations require detailed planning and integration equal to that required of EW operations conducted by ground units. Vital to successful air operations against modern air defenses.
- Airborne ES activities are usually conducted in general support of the MAGTF or the Joint Task Force (JTF).

- Non-organic platforms, specifically designed to perform EW, may be requested to support the MAGTF through JTF/theater commander.

c. Requirements.

- Clear understanding of the EW needs of the supported commander.
- Ground support facilities
- Liaison between the aircrews of the aircraft providing the EW support and the aircrews being supported.
- Protection from enemy aircraft

d. Capabilities.

- Airborne EW activities are ideally suited to directly support other tactical aviation missions.
- Extended EW range over that offered by ground assets.
- Possess greater mobility and flexibility than ground assets.
- Can support ground units or the MAGTF in general support in coordination with Radio Battalion.

e. Limitations.

- Limited assets.
- Time on station considerations.
- Vulnerable to enemy EP actions.
- Vulnerable to enemy electronic deception.
- Although the effective ranges at which ES and EA can be conducted by aircraft are far greater than those of ground EW assets, line-of-sight limitations (i.e., terrain masking and radar horizon) still apply.

EW and Joint Operations

Joint operations feature new command relationships and generally increase the complexity of EW operations. This is because coordination is more difficult because more agencies are involved in planning and execution. Although the structure will vary with the situation, the EW organization within the joint force normally centers on the joint force staff, component commands, the Joint commander’s electronic warfare staff (JCEWS), and supporting joint agencies.

The Joint Force Staff and EW

The Joint Force Staff Operations Director (J-3) has primary staff responsibility for EW activity and for planning, coordinating, and integrating joint EW operations with other combat disciplines. To assist the J-3 a JCEWS is normally formed. The Joint Force Staff Intelligence Director (J-2) is responsible for timely collection, processing, tailoring, and dissemination of all-source intelligence for EW. The Joint Force Staff Communications-Electronics Director (J-6) has primary staff responsibility for coordinating use of the entire electromagnetic spectrum for command and control (C2) systems and electronics dependent weapons systems employed by the joint force. A

joint force Information Operations (IO) Cell will normally be established to facilitate the broad coordination of EW and other IO disciplines.

Component Commands and EW

Operational control of EW assets is exercised through the component commanders. Each component is organized and equipped to conduct EW tasks in support of its basic missions and the JFC's campaign objectives. The JFC will normally designate a Joint Force Air Component Commander. The primary purpose for a JFACC is to provide unity of effort for employing air power in support of the JFC's objectives. The JFC specifies the JFACC's responsibilities and level of authority. Normally, the JFACC will be responsible for planning, coordinating, allocating, and tasking of air forces (including EW capable air assets) based on the JFC's apportionment decisions.

The JCEWS

A joint commander's electronic warfare staff (JCEWS) is formally established to support the joint force commander (JFC) in planning, coordinating, and integrating joint force EW operations. The JCEWS, as a staff element within the J-3, provides the joint focus for denying the enemy use of the electromagnetic spectrum while maintaining it availability for friendly use. The JCEWS coordinates closely with the joint force Information Operations Cell. The JCEWS ensures joint EW capabilities support the JFC's objectives.

The JCEWS is composed of representatives from each of the components making up the joint force and will be headed by an Electronic Warfare Officer (EWO) appointed by the J-3. The JCEWS includes representatives from the J-2 and J-6 to facilitate intelligence support and EW frequency de-confliction. Support teams from various organizations can be requested to assist the JCEWS.

Joint Agencies

Joint Operations Center (JOC)

The JFC normally organizes a Joint Operations Center to serve as the focal point for operational matters. The JOC battle staff, directed by the J-3, is comprised of representatives from the directorates within the joint headquarters (J-1, J-2, J-3 including the JCEWWS, J-6, etc).

Joint Intelligence Center (JIC)

The JIC is the focal point for the intelligence structure supporting the J-2. Directed by the J-2, the JIC communicates directly with the component intelligence agencies and monitors intelligence support to EW operations. The JIC has the capability to adjust intelligence gathering to support the EW mission.

Joint Frequency Management Office (JFMO)

The JFMO, within the J-6 directorate, is responsible for coordinating the C2 system use of the electromagnetic spectrum, frequency management, and frequency de-confliction. The JFMO develops the

frequency management plan and makes recommendations to alleviate mutual interference.

Joint Targeting Coordination Board (JTCB)

The JTCB typically reviews target information, develops targeting guidance and priorities, and may prepare and refine joint target lists. The JTCB monitors the effectiveness of targeting efforts, coordinates and de-conflicts all JTF targeting operations, validates no-fire areas, and approves new target nominations for inclusion in the joint target list.

EW and Multi-National Operations

US planners must be prepared to integrate US and allied or coalition EW capabilities into a single, integrated EW plan. They should also be capable of providing allied or coalition nations with information concerning US EW capabilities and provide EW support to allied or coalition nations. A fundamental task for the Electronic Warfare Officer (EWO) of a US-led multi-national force (MNF) is the recognize and resolve terminology and procedural issues. Fortunately, current NATO EW doctrine is largely based on US EW doctrine. Further, each element within a MNF must determine other participant's need to know and determine the releasability of EW related information to other allied or coalition forces. (See also, Joint Publication 3-51, *Joint Doctrine for Electronic Warfare*.)

MNF EW Organization

a. Multi-national Force Commander (MNFC). The multinational force commander provides guidance for planning and conducting EW operations to the MNF through the J-3 and the Information Operations (IO) Cell. The IO Cell serves as a forum to coordinate all IO related activities, including EW operations.

b. Multinational Staff. Within the multinational staff the J-3 has primary responsibility for the planning and integration of EW activities. A staff Electronic Warfare Officer (EWO) will be designated. His responsibilities include; ensuring the integration of allied/coalition augmentees, ensuring that EW plans and procedures are properly interpreted/translated, coordinating appropriate communications connectivity, and integrating allied/coalition communications into a Joint Restricted Frequency List (JRFL).

EW Mutual Support

a. Exchange of signals intelligence (SIGINT) information. Care should be taken not to violate SIGINT security rules when exchanging information.

b. Exchange of Electronic Order of Battle (EOB). In peacetime, this type of exchange is normally achieved under bilateral agreement. In MNF operations, the EWCC officer, through the theater Joint Analysis Center (JAC) or Joint Intelligence Center (JIC), should ensure the maintenance of an up-to-date EOB. Allied and coalition forces should be included consistent with information exchange guidelines.

c. EW Reprogramming. EW reprogramming is a national responsibility. However, the EWCC office should be aware of reprogramming efforts being conducted within the MNF. This includes the requirement to exchange information on the use of wartime reserve modes (WARM).

Annex X

Electronic Warfare Capabilities and Support Activities

Purpose

The purpose of this annex is to describe the organic EW capabilities of the MAGTF and present external EW support activities important to the MAGTF.

MAGTF Capabilities

To provide electronic warfare (EW) support, the Marine Corps has two types of EW units: Radio Battalion and Marine Tactical Electronic Warfare Squadrons (VMAQ).

Radio Battalion

a. Mission. The mission of radio battalion (RadBn) is to provide communications security (COMSEC) monitoring, tactical SIGINT, EW, and special intelligence (SI) communication support to the MAGTF.

b. Tasks. The radio battalion:

- Conducts interception, radio direction finding (DF), recording, and analysis of communications and non-communications signals and SIGINT processing, analysis, production, and reporting.
- Conducts EW against enemy or other hostile communications.
- Assists in the protection of MAGTF communications from enemy exploitation by conducting COMSEC monitoring, analysis, and reporting on friendly force communications.
- Provides special intelligence (SI) communications support and cryptographic guard (personnel and terminal equipment) in support of MAGTF command elements and RadBn operations. (Normally, the communications unit supporting the MAGTF CE provides communications connectivity for SI communications.)
- Provides task-organized detachments to MAGTFs with designated SIGINT, EW, SI communications, and other required capabilities.
- Exercises technical control and direction over MAGTF RadBn SIGINT and EW operations.
- Provides Radio Reconnaissance Teams (RRT) with specialized insertion and extraction capabilities (e.g., combat rubber raiding craft, fast rope, rappel, helocast, static line parachute) to provide specified SIGINT and limited EA support during advance force, pre-assault, or deep post-assault operations.
- Coordinates technical SIGINT requirements and exchanges SIGINT technical information and material with national, theater, joint, and other SIGINT units.
- Provides intermediate, third- and fourth-echelon maintenance of RadBn SIGINT and EW equipment.

c. Organization

1. Fleet Marine Force Units

The 1st RadBn, Marine Corps Base, Kaneohe Bay, Hawaii, is subordinate to Commander, Marine Corps Forces, Pacific (COMMARFORPAC), and supports both I and III MEFs. The 2nd RadBn, Camp Lejeune, North Carolina, is subordinate to II MEF. Both battalions are organized and equipped along functional lines to provide administrative control of subordinate elements, to facilitate training, and to permit rapid structuring and operational deployment of task-organized units or detachments.

2. Task Organization for MAGTF Support
An entire RadBn will support a MEF operation. To support smaller MAGTFs, the RadBn tactical organization is the task-organized SIGINT Support Unit (SSU). The SSU may be as large as a RadBn operational company or as small as a four-Marine team. The RadBn organization enables the rapid organizational deployment of task organized SSUs. See MCWP 2-15.2, *Signals Intelligence*.

A fully structured SSU containing all the capabilities found in a RadBn is comprised of six basic elements. The nature of the threat, specific mission tasking, and intelligence and operational requirements determine the composition and equipment of each element. The electronic attack (EA) element is comprised of the Marines and equipment to conduct EA operations. Personnel assigned to this element include EA supervisors or controllers and EA operators.

d. Ground EA Equipment

1. AN/ULQ-19(V)2 Electronic Attack Set. The AN/ULQ-19(V)2 electronic attack set provides the capability to conduct spot or sweep jamming of single channel voice or data signals operating in the standard military frequency range of 20-79.975 MHz from selected mobile platforms (e.g. HMMWVs, mobile EW support system (MEWSS), helicopters). When employed as a tactical, general-purpose, low-VHF jamming system, it has a 250-watt radio frequency linear amplifier that produces a nominal 200 watts of effective radiated power (ERP) using a standard omni-directional whip antenna. To provide required jamming, the system must be employed and operated from a location with an unobstructed signal line of sight to the target enemy’s communications transceiver.

2. AN/MLQ-36 Mobile Electronic Warfare Support System (MEWSS). The MEWSS provides a multi-functional capability that gives SIGINT/EW operators limited armor protection. This equipment is ideally suited to provide SIGINT/EW support for highly mobile mechanized and military operations in urban terrain where maneuver and/or armor protection is critical. MEWSS comprises a signals intercept system, a radio direction finding (DF) system, EA system, a secure communications system, and an intercom system installed in a logistics variant of the light armored vehicle (LAV).

3. AN/MLQ-36A Mobile Electronic Warfare Support System Product Improvement Program (MEWSS PIP). The MEWSS-PIP is an advanced SIGINT/EW system integrated into an LAV. The MEWSS-PIP provides a total replacement of the EW mission equipment now fielded in the AN/MLQ-36 MEWSS. The mission of the MEWSS PIP is to provide the MAGTF

with the capability to conduct Signals Intelligence (SIGINT) and Electronic Warfare (EW) operations using equipment mounted in a LAV. The MEWSS PIP provides the ability to detect and evaluate enemy communications emissions, detect and categorize enemy non-communications emissions (i.e., battlefield radars), determine Lines-of-Bearing (LOBs), and degrade enemy tactical radio communications during amphibious assaults and subsequent operations ashore. When mission configured, and working cooperatively with other MEWSS PIP platforms, the common suite of equipment can also provide precision location of battlefield emitters. The system is designed to have an automated tasking and reporting data link to other MAGTF assets such as the AN/TSQ-130 Technical Control and Analysis Center (TCAC) PIP. The MEWSS PIP and future enhancements will provide the capability to exploit new and sophisticated enemy electronic emissions and conduct Electronic Attack (EA) in support of existing and planned national, theater, Fleet, and MAGTF SIGINT/EW operations.

Marine Tactical Electronic Warfare Squadrons (VMAQs)

a. Mission and Tasks. VMAQs provide EW support to the MAGTF and other designated forces. To support the MAGTF, the VMAQ conducts tactical jamming to prevent, delay, or disrupt the detection and tracking of enemy early warning, acquisition, fire or missile control, counter-battery, and battlefield surveillance radars. Tactical jamming also denies and/or degrades enemy communications capabilities. In addition, the VMAQ conducts electronic reconnaissance and ES operations to maintain electronic orders of battle (EOB), to include both selected emitter parameters and location of non-friendly emitters. VMAQs also provide threat warnings for friendly aircraft, ships, and ground units. VMAQ tasks include:

- Provide airborne EA and ES support to ACE and other designated operations by intercepting, recording, and jamming threat communications and non-communication emitters.
- Processing, analyzing, and producing routine and time-sensitive ELINT reports for updating and maintaining enemy EOB. This is accomplished through the electronic warfare department, which includes intelligence, Tatical Eelctronic Reconnaissance Processing and Evaluation System (TERPES), and the Tactical EA-6B Mission Planning System (TEAMS). All are used to support pre-mission planning and post-mission processing of collected data and production of pertinent intelligence reports. Working in concert with squadron intelligence, TERPES and TEAMS provide required ELINT and EOB intelligence products to the ACE, MAGTF and other requesting external agencies.
- Providing liaison personnel to higher staffs to assist in VMAQ employment planning. Inherent in this task is the requirement to provide an air EW liaison officer to the MAGTF EWCC.
- Conduct EA operations for EP training of MAGTF units.

b. Organization and Concept of Employment. There are four VMAQs (designated VMAQ-1 through VMAQ-4) assigned to MAG-14, 2d MAW, Cherry Point, North Carolina. Each squadron has five EA-6B Prowler aircraft and is organized into administrative, intelligence and electronic warfare, operations, logistics, safety and standardization, and

maintenance divisions.

1. EA-6B Prowler. The EA-6B Prowler is a subsonic, all-weather, carrier-capable aircraft. The crew is composed of one pilot and three electronic countermeasure officers. The Prowler's primary missions include collecting and processing designated threat signals of interest (SOI) for jamming and subsequent processing, analysis, and intelligence reporting; and employing the AGM- 88 high-speed anti-radiation missile (HARM) against designated targets. The AN/ALQ-99 Tactical Jamming System effectively incorporates receivers and external pods for signals reception and transmission of jamming signals (principally those associated with threat air defense radars and associated C2). In addition to the AN/ALQ-99, the EA-6B also employs the USQ-113 communications jammer that provides the ability to collect, record, and disrupt threat communications.

2. Tactical EA-6B Mission Planning System (TEAMS). TEAMS is designed to assist EA-6B aircrew with planning and optimization of receivers, jammers, and HARM into a comprehensive package. TEAMS allows the operator to:

- Maintain area of operations emitter listings.
- Edit emitter parameters.
- Develop mission-specific geographic data and EOB.
- Perform post-flight mission analysis to:
  - Identify electronic emitters using various electronic parameter databases and ELINT analytical techniques.
  - Localize emitters by coordinates with a certain circular error of probability for each site.
  - Correlate new information with existing data.

3. Tactical Electronic Reconnaissance Processing and Evaluation System (TERPES). Each of the four VMAQ squadrons includes a TERPES section. The TERPES (AN/TSQ-90) is an air- and land-transportable, single-shelter ELINT processing and correlation system. The TERPES section is composed of Marines, equipment and software to:

- Identify and locate enemy radar emitters from data collected by EA-6B aircraft and those received from other intelligence sources.
- Process and disseminate EW data rapidly to MAGTF and other intelligence centers.
- Provide mission planning and briefing support.

(a) Operational Support. The TERPES will:

- Translate rapidly the machine-readable, airborne-collected digital data into man- and machine-readable reports (i.e., paper, magnetic tape, secure voice, plots, and overlays).
- Receive and process EA-6B mission tapes.
- Accept, correlate, and identify electronic emitters data from semiautomatic or automatic collection systems using various electronic parameter data bases and various analysis techniques.

- Provide tactical jamming analysis.

(b) Intelligence Analysis. The TERPES Intelligence Analysis Application (IAA) enables the operator to analyze ELINT data combined with additional modernized integrated database (MIDB) intelligence data to:

- Respond to intelligence requirements.
- Prepare intelligence database updates.
- Analyze threat and tactical situations.
- Estimate changes in the threat’s tactical situation.

(c) Data Fusion. MIDB is the primary intelligence data base for IAA operator queries. In addition to EA-6B aircraft mission tapes, other inputs may be fused to maximize the support provided to tactical intelligence operations to include:

- Naval intelligence database (NID) contains characteristics and performance data for weapons, sensors, and platforms.
- EWDS is similar to the NID and provides EA-6B tailored data.
- ELINT parameters list (EPL) is NSA’s observed radar parametric data.
- Electronic warfare integrated reprogramming (EWIR) is produced by the United States Air Force Foreign Technology Division. EWIR combines assessed technical radar parameters from the United States Air Force EW Science and Technology database with the observed parameters of the NSA database.
- Joint Spectrum Center (JSC) is used to derive friendly EOB and radar parametric data.

(d) TERPES Fusion Processor. The TERPES fusion processor (TFP) processes intelligence data from tactical ELINT (TACELINT) reports, Sensor Reports (SENSOREPS), tactical reports (TACREPs), and imagery intelligence (IMINT) reports. The TFP provides filtering, characteristic and performance identification, order of battle (OOB) identification, technical analysis, multi-source correlation, and candidate updates. The TFP presents the information in various forms for analysis. One TFP integrated information on source is the Tactical Related Applications Processor Data Dissemmination System (TDDS) Broadcast. This broadcast is accessed using the Commander’s Tactical Terminal (CTT) and provides near-realtime (NRT), national-level reports to the TERPES. The TDDS broadcast also assists the TFP in maintaining an ELINT parameter database to track airborne, shipboard, and land-based targets as a tool to develop EOBs and as an instrument to perform comparative studies on radar parameters.

(e) TERPES ELINT Preprocessor. The TERPES ELINT preprocessor (TEPP) processes all EA-6B signals of interest (SOIs) collected from recorder or reproducer set tape or disk files.

Specifically, the application allows for the NRT analysis of technical ELINT data. Position reports and specific unit identification and location information are used to update the TERPES database and to prepare TACELINT reports. TERPES also provides tactical jamming system (TJS) analysis for the EA-6B aircrew and maintenance personnel. TJS analysis consists of recovering recorded data for verifying jammed calibration, jammer on and off times, and frequency and azimuth coverage. TERPES will use mission data in the generation of EW mission summary reports.

4. Intelligence Reporting

The primary intelligence output from TERPES is in the form of post-mission reports. Post-mission reports are available in many forms and are provided intelligence elements in response to established intelligence requirements. The most commonly used reporting form is the TACELINT (refer to USSID 340, *Tactical ELINT Reporting*, for format and content). Other report forms include the following:

- TACREP provides information on immediate threat activity.
- ELINT summary report provides a summary of ELINT activity over established periods (normally 24 hours). Refer to USSID 200, *Technical SIGINT Reporting*, for format and content.
- ELINT technical report provides for analyst exchange of information of parametric data. Refer to USSID 341, *Technical ELINT Reporting*, for format and content.
- Over the horizon (OTH) “GOLD” report provides information derived from contact reports of ELINT parametrics.
- Order of battle report (OBREP) provides order of battle information such as basic encyclopedia (BE) number, equipment, and location.

External Support Activities

JIOC. The JIOC was originally activated as the Joint Electronic Warfare Command (JEWC) and re-designated as the Joint Command and Control Warfare Center (JC2WC) in October 1994. Re-named the Joint Information Operations Center (JIOC) in September 1999, the JIOC in San Antonio, Texas provides a valuable resource for the Commanders of the Combatant Commands (CINCs). The JIOC is fully engaged in the warfighting application of IW. The JIOC dispatches tailored teams to augment CINC and Joint Task Force staffs and provide IO/IW expertise in all joint exercises and contingency operations.

The JIOC also has EW Reprogramming oversight responsibilities for the joint staff. Oversight responsibilities include requirements to organize, manage, and exercise joint aspects of EW reprogramming and facilitate the exchange of data used in joint EW reprogramming. However, actual reprogramming of equipment is a Service responsibility.

Joint Spectrum Center. The DOD Joint Spectrum Center (JSC) was activated in September 1994 under the direction of the Joint Staff J6. The JSC assumed all the mission and responsibilities previously performed by the Electromagnetic Compatibility Center, as well as

additional functions. The Joint Spectrum Center (JSC) has assembled leading experts in spectrum planning, electromagnetic compatibility (EMC)/vulnerability (EMV), electromagnetic environmental effects (E3), information systems (IS), modeling and simulation, operations support, and system acquisition to provide complete, spectrum related services to the CINCs, Military Services, and other Government organizations.

The JSC deploys teams in support of the Commanders-In-Chief (CINCs) and serves as the DOD focal point for supporting spectrum supremacy aspects of IW. Notably the JSC assists warfighters in developing and managing the Joint Restricted Frequency List (JRFL) and assisting in the resolution of operational interference and jamming incidents. The JSC can provide databases on friendly force C2 systems for use in planning C2-protect.

Joint COMSEC Monitoring Activity. The Joint COMSEC Monitoring Agency (JCMA) was created in 1993 by a Memorandum of Agreement between the Service Operations Deputies, Directors of the Joint Staff, and NSA. The JCMA is charged with conducting "COMSEC monitoring (collection, analysis, and reporting) of DOD telecommunications and automated information systems (AIS) and monitoring of related non-communications signals." Its purpose is to identify vulnerabilities exploitable by potential adversaries and recommend countermeasures and corrective actions. The JCMA supports both real-world operations, as well as joint exercises and DOD systems monitoring.

Joint Warfare Analysis Center. Located in Dahlgren, Virginia the Joint Warfare Analysis Center (JWAC) assists commanders in their preparation and analysis of joint operations plans. The JWAC provides analysis of engineering and scientific data and integrates operational analysis with intelligence.

Applied Physics Laboratory. The Applied Physics Laboratory (APL) is a not-for-profit R&D division of The Johns Hopkins University. APL is organized into a federation of sponsored technical and service departments, under Central Laboratory Office direction. As a matrix management organization, APL often employs the resources of multiple departments for specific program and technical needs.

National Security Agency. The National Security Agency (NSA) is the Nation's cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information. A high technology organization, NSA is on the frontiers of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the Government.

Naval Security Group Command. The responsibilities of the Commander, Naval Security Group Command (NSGC) in regard to Marine Corps participation in Department of Navy cryptologic activities are determined by mutual agreement between CNO and the Commandant of the Marine Corps. The NSGC acts as Executive Agent for the Department of the Navy and coordinates with the NSA and other Department of Defense and national agencies on cryptology matters; reviews and appraises the implementation of approved cryptology plans and programs. It provides support and technical guidance to the operating forces of the Navy on cryptologic matters; supports and provides technical guidance for electronic warfare programs and operations, as required. The NSGC

prioritizes Department of the Navy conduct and support of cryptologic operations as authorized and directed by the Secretary of Defense, including reserve programs to meet emergency or wartime requirements for cryptologist resources.

APPENDIX XXX

JOPES ELECTRONIC WARFARE GUIDANCE

Purpose. The purpose of this appendix is to provide a basic framework for the development of EW guidance.

EW Guidance. EW guidance relates to the development of Tab B (Electronic Warfare) of Appendix 3 (Information Warfare) to Annex C (Operations) of the format found in CJCSM 3122.03, *"Joint Operation Planning and Execution System Volume II: (Planning Formats and Guidance)".*

1. Situation

a. Enemy Forces

What are capabilities, limitations, and vulnerabilities of enemy communications, non-emitting, and EW systems?
What is the enemy capability to interfere with accomplishment of the EW mission?

b. Friendly Forces

What friendly EW facilities, resources, and organizations may affect EW planning by subordinate commanders?
Who are the friendly foreign forces with which subordinate commanders may operate?

c. Civilian and/or Neutral Facilities

What civilian and/or neutral facilities, resources, and organizations may affect EW planning by subordinates?
What potential collateral effects could be expected?

d. Assumptions.

What are the assumptions concerning friendly or enemy capabilities and COAs that significantly influence the planning of EW operations?

2. Mission

What is the EW mission (who, what, where, when, why)?

3. Execution

a. Concept of Operations

What is the role of EW in the commander's strategy?
What is the scope of EW operations?
What methods and resources will be employed? Include organic and non-organic capabilities.
How will EW support the other elements of IO and SEAD?

b. Tasks. What are the individual EW tasks and responsibilities for each component or subdivision of the force? Include all instructions unique to that component or subdivision.

c. Coordinating Instructions

What instructions, if any, are applicable to two or more components or subdivisions?

What are the requirements, if any, for the coordination of EW actions between subordinate elements?

What is the guidance on the employment of each activity, special measure, or procedure that is to be used but is not covered elsewhere in this tab?

What is the emissions control (EMCON) guidance? Place detailed or lengthy guidance in an exhibit to this tab.

What coordination with the J-6 (or G/S-6) is required to accomplish the JRFL?

4. Administration and Logistics

a. Administration

What, if any, administrative guidance is required?
What, if any, reports are required? Included example(s).

b. Logistics. What, if any, are the special instructions on logistic support for EW operations?

5. Command and Control

a. Feedback

What is the concept for monitoring the effectiveness of EW operations during execution?
What are the specific intelligence requirements for feedback?

b. After-Action Reports. What are the requirements for after-action reporting?

c. Signal. What, is any, are the special or unusual EW-related communications requirements?

APPENDIX XXX

JOPES ELECTRONIC WARFARE APPENDIX FORMAT

SECURITY CLASSIFICATION

ISSUING HEADQUARTERS
LOCATION
DAY, MONTH, YEAR, HOUR, ZONE

TAB B ELECTRONIC WARFARE TO APPENDIX 3 INFORMATION OPERATIONS ANNEX C OPERATIONS TO XXXXXX OPLAN XXXX-XX (U)

(U) References: List basic documents required

1. ( ) Situation

a. ( ) Enemy. Refer to annex B. Provide an estimate of enemy communications, non-communications, and EW systems capabilities, limitations, and vulnerabilities, including the ability to interfere with the accomplishment of the EW mission.

b. ( ) Friendly. Provide a summary of friendly EW facilities, resources, and organizations that may affect EW planning by subordinate commanders. Include friendly foreign forces with which subordinate commanders may operate.

c. ( ) Assumptions. State any significant assumptions about friendly or enemy capabilities and course of action that significantly influence the planning of EW operations.

2. ( ) Mission. State the mission to be accomplished by EW operations to support the mission in the basic plan.

3. ( ) Execution

a. ( ) Commander’s Intent.

b. ( ) Concept of Operations. Summarize the scope of EW operations and the methods and resources to be employed. Include the employment of organic and non-organic capabilities.

c. ( ) Tasks. In separate numbered sub-paragraphs, assign individual EW tasks and responsibilities to each component or element of the joint force or MAGTF, including all instructions that are unique to that component.

d. ( ) Coordinating Instructions

(1) ( ) Place instructions applicable to two or more components or elements in the final sub-paragraph.

(2) ( ) Include instructions for coordination with the support of deception, unconventional warfare, PSYOP, SIGINT activities etc.

4. ( ) Guiding Principles. State or refer to policies, doctrine, and procedures published elsewhere that provide guidelines to be followed on implementing this plan. Establish any additional guiding principles to be followed, as well as authorized deviations from standard practices. Describe any EW constraints that apply to the operations.

5. ( ) Special Measures. Provide guidance on the employment of each activity, special measure, or procedure that is to be used but is not covered in this annex.

6. ( ) Administration and Logistics

a. ( ) Logistics. Provide special instructions pertaining to logistic support for EW operations.

b. ( ) Administration. Include necessary administrative guidance.

(1) ( ) Provide guidance when modifications to Service EMI reporting instructions are necessary.

(2) ( ) Provide for timely operations reporting system (OPREP) reporting of EW activities.

7. ( ) Command and Signals

a. ( ) Command. Designate lead EW activity.

b. ( ) Signals. Define EW reporting requirements.

ANNEX XXX

JOINT ELECTRONIC WARFARE REPORTS

Purpose: The purpose of this appendix is to identify significant joint EW reports, briefly describe their purpose, and identify report originators and addressees.

Joint EW Reports: Joint publications set forth approved procedures and formats for standardizing EW message traffic in joint operations. CJCSM 6120.05 *(Tactical Command and Control Planning Guidance for Joint Operations, Joint Interface Operational Procedures For Message Text Formats)* presents implementation of United States Message Text Formats (USMTFs).

The tabs to this appendix describe EW or EW related messages that may be to support EW operations. Addresses/ originators listed are samples. Specific addresses/originators are situation dependent and are revised periodically. The appropriate reference for detailed formats and data requirements is included in the description. Note: A sample format for the EW frequency de-confliction message (extracted from Joint Spectrum Management System (JSMS)) is included as an exhibit to Tab L.

Message	USMTF Short Title	Tab
EW Mission Summary	EWMSNSUM	A
EW Employment	EWEM	B
EW Approval	EWAM	C
Tactical Report	TACREP	D
EW Requesting or Tasking Message	EWRTM	E
Tactical Electronics Intelligence Report	TACELINT	F
EA Data	EADAT	G
SIGINT, EA Planning, & Coordination	SIEPCM	H
ELINT Requirement Tasking Message	ERTM	I
Air Support Request	AIRSUPREQ	J
Air Request Jammer	AIRREQJAM	K
EW Frequency Deconfliction	EWDECONFLICT	L
MIJI Feeder Report	MIJIFEEDER	M
Sensitive Information Report	SIREP	N
Stop Jamming Message	STOP JAMMING	O

TAB A

EW MISSION SUMMARY (EWMSNSUM)

1. Purpose. The EWMSNSUM is used to summarize significant EW missions and the status of offensive EW assets. The EWMSNSUM will not be used to report the results of ES operations. The TACREP will be used to report ES operational results.

2. Originator. TOC, AOC, MAGTF COC.

3. Addressee. JOC (record only), TOC, AOC, MAGTF COC.

4. Method of Transmission. When EWMSNSUM is sent to the JOC, it is sent by record only. When sent cross-Service, the primary method of transmission is record with voice as an alternate. The message preparer may use any one or all of the formatted sets when reporting the EW summary activity.

5. Frequency of Transmission and Update. As required, as specified in OPLAN, or in accordance with established operations plans for the theater of operations.

6. Procedures. EWMSNSUM is used by all EW/EA capable surface and air units to provide information on EW operations. It is used by the Service component commanders to report significant events for subsequent analysis.

TAB B

EW EMPLOYMENT MESSAGE (EWEM)

1. Purpose. The EWEM is used to provide the COMJTF with the component commander's intentions for the employment of EA for either a specific reporting period or for a specific EW mission. Reporting requirements are to be established by the COMJTF. The EWEM is used by the JOC to eliminate potential EW mission conflicts. It may also be used by component commanders to warn or notify of intended EA actions.

2. Originator. TOC, EWC, OTC/CWC/CATF, AOC, MAGTF COC, AFSOD.

3. Addressee. JOC, TOC, OTC/CWC/CATF, AAWC, ASWC, ASUWC, EWC, AOC, MAGTF COC, JOC(SOC/JSOTF), NSWTG, SFOB

4. Method of Transmission. The primary method of transmission is record with voice as alternate.

5. Frequency of Transmission or Update. As established by the COMJTF OPLAN, as required to reflect a Service component's EW intentions, or as required to respond to an EWRTM.

6. Procedures. The EWEM can simply reflect a component commander's intentions for EA employment; but as the required response to an EWRTM, the EWTM also contains the component's planned EW support.

TAB C

EW APPROVAL MESSAGE (EWAM)

1. Purpose. The EWAM is used by the COMJTF to approve or modify the total joint operations EW plan.

2. Originator. JOC

3. Addressee. TOC, AAWC, ASWC, ASUWC, EWC, OTC/CWC/CATF, AOC, MAGTF COC

4. Method of Transmission. The primary method of transmission is record with voice as alternate.

5. Frequency of Transmission or Update. As required.

6. Procedures. The COMJTF references the component's message, identifies the applicable time frame, and approves, disapproves, or modifies EW tasking. If disapproved or modification is directed, amplifying details are forwarded. When no conflicts exist in the component commander's EW schedule and the overall EW plan satisfies joint mission objectives, the EWAM will simply state "approved." If changes, cancellations, or modifications to the joint operations EW plan are required, the JOC will so state and send the EWAM to the appropriate component. The component can adjust his schedule as directed through the normal tasking cycle. Blanket EA restrictions (such as jam-free frequencies) will be provided via the ORDER or PLANORDCHG message. Control measures (such as "stop EA") will be handled by standard voice procedures and not by this message.

TAB D

TACTICAL REPORT (TACREP)

1. Purpose. The TACREP is used only to provide perishable information of tactical significance, for the immediate attention of the tactical commander.

2. Originator. JIC (JTF), ASAC, AAWC, ASWC, ASWOC, ASUWC, EWC, FOSIC, OTC/CWC/CATF, SUBOPCONCEN, E-3, DSU (AF), AOC-INTEL, WOC-F, RADBN DET, MAGTF-INTEL, JOC (SOC/JSOTF), AFSOD, AFSOE, FOB, NSWTG, NSWTU, SFOB

3. Addressee. JIC (JTF), DIA, ASAC, AAWC, ASWC, ASWOC, ASUWC, EWC, FCC, FOSIC, OTC/CWC/CATF, SBOPCONCEN, AME, DSU (AF), E-3, AOC-INTEL, WOC-F, RADBN DET, MAGTF-INTEL, JOC (SOC/JSOTF), AFSOD, AFSOE, FOB, NSWTG, NSWTU, SFOB

4. Method of Transmission. The primary method of transmission is record with voice as alternate. GENSER OR SCI channels are used as appropriate. The TACREP is normally sent with an IMMEDIATE or FLASH precedence because of the high priority and perishable nature of the information.

5. Frequency of Transmission or Update. As required.

6. Comments. The TACREP is used to alert commanders of immediate threats to friendly forces. Amplifying information may be reported by other message formats (for example, INTREP, SIREP). Because of the significance of this report, the message should not be delayed to obtain all possible data on a continuing event. For maritime operations reporting, the TACREP is used to report contacts developed by HFDF assets.

CAUTION: Since the TACREP is the primary message text format used for reporting time critical intelligence information, it can be sent by any C2/Information Exchange element in addition to those identified in paragraph 2 above. It is essential that all C2 element watchstanders be familiar with the TACREP content and interface procedures.

TAB E

EW REQUESTING OR TASKING MESSAGE (EWRTM)

1. Purpose. The EWRTM is used by the COMJTF to task component commanders to perform EW operations in support of the overall joint EW plan and to support component EW operations, and also used by component commanders to request EW support from sources outside their command.

2. Originator. JOC, TOC, EWC, OTC/CWC/CATF, AOC, MAGTF COC, JOC (SOC/JSOTF)

3. Addressee. JOC, TOC, AAWC, ASWC, ASUWC, EWC, FOSIC, OTC/CWC/CATF, AOC, MAGTF COC, AFSOD

4. Method of Transmission. The primary method of transmission is record with voice as an alternate.

5. Frequency of Transmission or Update. As required.

6. Procedures. The EWRTM will not be used to request or task support from SIGINT assets. Mission coordination details and additional specific equipment parameters will be exchanged using messages such as the SIEPCM. Requesting numbering will be in accordance with JTF OPLANs or OPORDs. The COMJTF's tasking or Service component commanders's request (EWRTM) will be responded to by the Electronic Warfare Employment Message (EWEM).

TAB F

TACTICAL ELECTRONICS INTELLIGENCE REPORT (TACELINT)

1. Purpose. The TACELINT is used to report time-critical operational ELINT and parametric information. Information contained therein may be used for indications and warning, data base maintenance, orders of battle, and strike planning. ELINT collectors use this message format as a reporting vehicle. The COMJTF uses this message format to advise the joint force of updates to the ELINT order of battle or data base.

2. Originator. JIC(JTF), AAWC, ASWC, ASUWC, EWC, FOSIC, OTC/CWC/CATF, II(AF), TEP, RADBN DET, MAGTF-INTEL, TERPES

3. Addressee. JIC(JTF), DIA, ASAC, AAWC, ASWC, ASWOC, ASUWC, EWC, FCC, FOSIC, OTC/CWC/CATF, SUBOPCONCEN, DSU(AF), AOC-INTEL, RADBN DET, MAGTF-INTEL, TERPES

4. Method of Transmission. The primary method of transmission is record. Voice transmission is a backup for ASAC, JIC interface and the SCI-capable C2/Information Exchange elements. General services/special compartmented information (GENSER/SCI) channels are used as appropriate.

5. Frequency of Transmission or Update. As required.

6. Comments. The TACELINT report advises joint forces of changes and updates to the ground, naval, or air electronics orders of battle (EOBs). This message will be prepared whenever vital information information is obtained. The COMJTF may designate an internal or external organization to maintain the JTF ELINT database. This will be published in the JTF letters of instruction and/or OPLANs, and the designated organization will be an information addressee on all ELINT message traffic.

TAB G

EA DATA MESSAGE (EADAT)

1. Purpose. The EADAT is used to report EA strobe data in the absence of a TADIL A or TADIL B link.

2. Originator. ADACP, AAWC, OTC/CWC/CATF, CRC/CRP, DSU(AF), E-3, TACC/TADC(M), TAOC

3. Addressee. ADACP, AAWC, OTC/CWC/CATF, CRC/CRP, DSU(AF), e-3, TACC/TADC(M), TAOC, ABCCC

4. Method of Transmission. Voice only.

5. Frequency of Transmission or Update. As required to report an EA signal. Update every 5 minutes until location of jamming has been determined.

6. Comments. This message is used to report an EA strobe from an affected or detecting unit's position to an aircraft emitting EA. It is used to determine the location of a hostile or unknown aircraft emitting EA. It is reported by the detecting unit to all units on a net when the data link is degraded or not operational. After receipt of several electronic attack data (EADAT) messages, it is possible to determine the source of enemy EA by comparing lines of bearing from the different origins. Once this is accomplished, the EA aircraft can be engaged with friendly interceptors or surface-to-air missiles (SAMs). Requirement for the EADAT terminates when the EA source is destroyed, the EA ceases, or the TADIL reporting is restored. As soon as the tactical situation allows, a MIJIFEEDER report should be submitted.

TAB H

SIGINT, EA PLANNING, AND COORDINATING MESSAGE (SIEPCM)

1. Purpose. The SIEPCM is used to plan and coordinate SIGINT collection and EA communications or noncommunications missions. It is also a vehicle for requesting cross-Service assets to satisfy tasks beyond a component Service's capabilities.

2. Originator. JIC(JTF), ASAC, ASWC, ASUWC, EWC, FOSIC, OTC/CWC/CATF, DSU(AF), RADBN DET

3. Addressee. JIC(JTF), DIA, ASAC, AWUWC, EWC, OTC/CWC/CATF, DSU(AF), RADBN DET

4. Method of Transmission. Record only; SCI only.

5. Frequency of Transmission or Update. As required.

6. Comments. Service component planners will use this message to resolve and/or preclude EA/EP mutual interference problems and to maximize SIGINT/EA resource coverage within the JTF's area of responsibility (AOR). The JTF's headquarters will incorporate the information from this message into the planning process. Each component's request for assistance beyond their capability will be sent to the COMJTF with justification. Unless otherwise directed, the SIEPCM or MSGCORRCANXs submitted subsequent to the initial message will normally report only modification to the previous SIEPCM.

TAB I

ELINT REQUIREMENT TASKING MESSAGE (ERTM)

1. Purpose. The ERTM is used by operational commanders to task resources under their OPCON for the purpose of ELINT collection, or to request ELINT collection from sources outside of their OPCON.

2. Originator. JIC(JTF), ASAC, DSU(AF), AOC-INTEL, RADBN DET, MAGTF-INTEL, TERPES

3. Addressee. JIC(JTF), DIA, ASAC, EWC, OTC/CWC/CATF, DSU(AF), AOC-INTEL, RADBN DET, MAGTF-INTEL, TERPES

4. Method of Transmission. Record only. Transmission channels are GENSER or SCI as appropriate.

5. Frequency of Transmission or Update. As required.

6. Comments. Component commanders submit the ERTM to the COMJTF (JIC(JTF)) when requesting ELINT collection outside their operational control. If the COMJTF approves the request, COMJTF (JIC(JTF)) will submit an ERTM to the appropriate source internal or external to the joint force.

TAB J

AIR SUPPORT REQUEST (AIRSUPREQ)

1. Purpose. Used to request preplanned and immediate close air support, interdiction, reconnaissance, surveillance, escort, helicopter airlift, and other aircraft missions.

2. Originator. TOC, ASAC, ASWC, OTC/CWC/CATF, ABCCC, AOC, DASC, TACC/TADC(M), JOC(SOC/JSOTF), AFSOD, AFSOE, FOB, NSWTG, NSWTU, SFOB

3. Addressee. JFACC (if desired), JOC, FCC, OTC/CWC/CATF, ASOC, ABCCC, AOC, DASC, MAGTF COC, TACC/TADC (M), JOC(SOC/JSOTF)

4. Method of Transmission. The primary method is record with voice as an alternate. The voice message is normally used for immediate requests when the time-on-target is less than 6 hours form the time of the request. COMJTF may designate the non-JNTACCS format be used in place of the AIRSUPREQ voice formats.

5. Frequency of Transmission or Update

a. Preplanned. The AIRSUPREQ must be submitted in time to the supporting component so each component is able to include the request in its daily air allocation request to the JFACC, if designated.

b. Immediate. As required to request immediate air support.

6. Comments. The AIRSUPREQ can be used to request air support directly from the other Service components, if authorized, or from other components through the JFACC, if designated.

TAB K

AIR REQUEST JAMMER (AIRREQJAM)

1. Purpose. The AIRREQJAM is used to request preplanned and immediate EW air support missions. This message is transmitted by voice only.

2. Originator. ASAC, TOC, ASWC, OTC/CWC/CATF, ABCCC, AOC, DASC, TACC/TADC (M).

3. Addressee. JFACC (if designated), JOC, TOC, FCC, OTC/CWC/CATF, ASOC, ABCCC, AOC, DASC, TACC/TADC (M).

4. Method of Transmission. Voice only; it is a backup to the AIRSUPREQ record message.

5. Frequency of Transmission or Update. As required.

6. Comments. The AIRREQJAM is used as a backup means to the AIRSUPREQ record message for preplanned and immediate air support, or when timely dissemination of information precludes record message formatting.

TAB L

EW FREQUENCY DECONFLICTION MESSAGE (EWDECONFLICT)

1. Purpose. The EWDECONFLICT is used to promulgate a list of PROTECTED, GUARDED, and TABOO frequencies, for inclusion in the JRFL, so as to ensure friendly force use of the frequency spectrum without adverse impact from friendly EA.

2. Originator. JOC

3. Addressee. TOC, OTC/CWC/CATF, AOC, MAGTF COC

4. Method of Transmission. Record with voice as an alternate. Transmission channels are GENSER or SCI as appropriate.

5. Frequency of Transmission or Update. The JRFL is constantly being modified and a EWDECONFLICT is needed (at least daily) to protect frequencies from being jammed or other forms of manipulation.

6. Comments. The EWDECONFLICT provides a rapid and efficient means to transmit changes to the JRFL. The JRFL is the only authorized mechanism through which the Department of Defense can protect frequencies from jamming or other forms of manipulation.

TAB M

MEACONING, INTRUSION, JAMMING, AND INTERFERENCE FEEDER REPORT (MIJIFEEDER)

1. Purpose. The MIJIFEEDER is used as a primary means of sharing MIJI incidents in a timely manner, and provides for joint exchange of tactical MIJI information, including electro-optic interference.

2. Originator. JIC(JTF), AAWC, ASWC, ASWOC, ASUWC, EWC, FOSIC, OTC/CWC/CATF, AOC-INTEL, WOC-F, WOC-R, WOC-A, RADBN DET, MAGTF-INTEL, TERPES, JOC(SOC/JSOTF), AFSOD, AFSOE, FOB, NSWTG, NSWTU, SFOB

3. Addressee. JIC(JTF), DIA, ASAC, AAWC, ASWC, ASWOC, ASUWC, EWC, FCC, FOSIC, OTC/CWC/CATF, SUBOPCONCEN, AME, AOC-INTEL, WOC-F, WOC-R, WOC-A, RADBN DET, TERPES, MAGTF-INTEL, JOC(SOC/JSOTF), AFSOD, AFSOE, FOB, NSWTG, NSWTU, SFOB

4. Method of Transmission. Primary method is record with voice as alternate; GENSER.

5. Frequency of Transmission or Update. As soon as any MIJI incident occurs. Use "IMMEDIATE" precedence.

6. Comments. A MIJIFEEDER message should be sent even when in doubt about any unknown interference. A MIJIFEEDER can help resolve friendly mutual interference. The COMJTF will coordinate if the reported MIJI incident was caused by external sources.

TAB N

SENSITIVE INFORMATION REPORT (SIREP)

1. Purpose. The SIREP is used to provide sensitive information on events or conditions that may have a significant impact on current planning of an operation, but of less time criticality than a TACREP. This message provides a sensitive file maintenance update mechanism.

2. Originator. JIC(JTF), DIA, ASAC, DSU(AF), RADBN DET.

3. Addressee. JIC(JTF), DIA, ASAC, AAWC, ASWOC, FCC, FOSIC, OTC/CWC/CATF, SUBOPCONCEN, DSU(AF), RADBN DET

4. Method of Transmission. Record; SCI only.

5. Frequency of Transmission or Update. As required.

6. Comments. The SIREP may be used to supplement information disseminated in other reports; e.g. TACREP, ITREP. When used in this capacity, the reference set of the SIREP must identify the original message. A SIREP reports information that affects planning rather than execution actions. The SIREP may also be a feeder report for the SISUM.

TAB O

STOP JAMMING MESSAGE (STOP JAMMING)

1. Purpose. The STOP JAMMING Message is used to terminate a jamming task being conducted by an EA asset.

2. Originator. Any established command and control and intelligence element.

3. Addressee. Next higher headquarters and any established command and control and intelligence element.

4. Method of Transmission. Record, voice back0up. GENSER. Voice becomes primary if record is disrupted.

5. Frequency of Transmission or Update. As required.

6. Comments. The STOP JAMMING message is used by the COMJTF to stop friendly jamming operations, when those operations are affecting the joint information flow. It is used by any element to request termination of friendly jamming operations that are affecting their information flow. The use of this message does not relieve the originator from the requirements of submitting a MIJIFEEDER report.